

# Verteidigung in der Vielfalt

**Know-how** Die klassische Perimetersicherheit ist in den meisten Organisationen überholt. Wie Netzwerksicherheit für verteilte und heterogene Unternehmenslandschaften und mit mobilem Arbeiten in Einklang gebracht werden kann.

Von Patrick Trevisan

Nie zuvor war die Unternehmens-IT derart dezentral und heterogen wie heute. Mehrere Standorte, flexible Geschäftsmodelle sowie der Siegeszug von Home Office und mobilem Arbeiten machen klassische Schutzkonzepte obsolet. Der Schutz von Netzwerkstrukturen, Daten und Nutzeridentitäten ist nicht allein eine Frage einzelner Technologien. Es braucht eine ganzheitliche Strategie, die fortlaufend neu ausgerichtet werden muss. Zu den grössten Herausforderungen zählen zum einen heterogene Netzwerke. Denn Unternehmen setzen unterschiedlichste Systeme, Endgeräte und Infrastrukturen ein – von Windows, MacOS und iOS über Android bis hin zu proprietären Cloud-Lösungen. Die ständige Anpassung an neue digitale Arbeitsweisen

und Bedrohungen macht diese Komplexität an sich zum Hauptproblem. Hinzu kommt die Zunahme hybrider und mobiler Arbeitsformen; Mitarbeitende greifen von zuhause, unterwegs oder von wechselnden Offices auf zentrale Ressourcen zu. Der Perimeter ist damit abgeschafft, denn die Angriffsflächen verteilen sich über Standorte und Anbieter hinweg. Des Weiteren spielen Regulatorik und Compliance eine wichtige Rolle, erfordern doch Datenschutz, Schweizer Vorgaben und branchenspezifische Regularien Kontrolle und protokollierte Absicherung sämtlicher Datenströme. Und schliesslich nimmt ganz allgemein die Bedrohung ständig zu: durch KI-gestützte Angriffe, gezieltes Phishing und die Ausnutzung von Schwachstellen in BYOD- und Multi-Betriebssystemumgebungen.

Kommunikationsbeziehung segmentiert werden. Kernbestandteile dabei sind zwingend Multi-Faktor-Authentifizierung für alle Nutzenden und Geräte, eine granulare Verteilung von Ressourcen und Zugriffsrechten (Mikrosegmentierung) sowie automatisierte Echtzeitüberwachung sämtlicher Endgeräte, Netzwerkverbindungen und Datenzugriffe.

## 2. Cloud-delivered Security und Security Operations Center

Moderne Security-Plattformen erlauben eine zentrale Steuerung und Überwachung aller Netzwerkteilnehmer durch ein SOC (Security Operations Center) unabhängig von Standort und Endgerät. Mit cloudbasierten Technologien wie Next-Generation-Firewalls und Managed Security Services können Unternehmen flexibel reagieren: Diese umfassen eine dynamische Policy-Steuerung für jedes Gerät und alle Nutzenden, die flexible Einbindung unterschiedlicher Betriebsplattformen, KI-gestützte Bedrohungsanalyse und einen Incident-Response-Plan. Letzterer definiert die notwendigen Schritte und Zuständigkeiten im Unternehmen für eine schnelle, koordinierte Reaktion auf IT-Sicherheitsvorfälle, um Cyberangriffe oder Datenverluste rasch zu erkennen, einzudämmen, zu analysieren und die Systeme wiederherzustellen. Ziel ist es, Schäden und Betriebsunterbrechungen für das Unternehmen zu minimieren und aus Vorfällen zu lernen, um zukünftige Bedrohungen besser bewältigen zu können. Um von Windows über Android bis iOS und MacOS für alle Betriebssystem-

### BEST PRACTICES FÜR MOBILE SICHERHEIT IN KÜRZE

- Schnelle Integration neuer Standorte und Home-Office-Arbeitsplätze via cloud-delivered Security und automatisierter Policy-Steuerung
- MDM/MTD-Hybridssysteme für die plattformübergreifende Sicherheit und Compliance-Überwachung
- Zero Trust und Microsegmentierung als Grundprinzip für die Zugriffssteuerung und Incident Prevention
- BYOD- und COPE-Richtlinien mit klarer Trennung, Rechtevergabe und automatischem Reporting
- Intensive Schulungsmassnahmen und Awareness-Programme für alle Mitarbeitenden

### Technologische Lösungsansätze

Um diesen umfassenden Herausforderungen zu begegnen, muss der Einsatz unterschiedlicher Technologien mittels eines mehrschichtigen Sicherheitskonzepts erfolgen. Ziel dabei ist, Zugriffe konsequent zu authentifizieren, Bedrohungen mithilfe von KI-Lösungen und Echtzeitüberwachung frühzeitig zu erkennen und Geräte standortunabhängig mit einheitlichen Sicherheitsrichtlinien zu schützen. Die Kombination dieser Ansätze reduziert die Angriffsfläche und ermöglicht eine schnelle, koordinierte Reaktion auf Sicherheitsvorfälle.

#### 1. Zero Trust Network Access

Das Zero-Trust-Modell geht davon aus, dass innerhalb und ausserhalb des Netzwerks nichts und niemand per se vertrauenswürdig ist. Jeder Zugriff muss deshalb authentifiziert, jede

teme die gleiche Sicherheit zu gewährleisten, müssen Unternehmen auf Plattformen setzen, die Zentralisierung und Granularität verbinden. Security Policies müssen betriebssystemübergreifend ausgerollt und überwacht werden. Geräte müssen inventarisiert, Schwachstellen analysiert und automatisch in Quarantäne gesetzt werden können.

### 3. Mobile Device Management (MDM)

Die Verwaltung und Absicherung diverser Geräte (Windows, Android, MacOS und iOS) ist damit der Schlüssel zur Reduktion der Angriffsflächen. Ein MDM-System (Mobile Device Management) steuert betriebssystemübergreifend, verteilt Richtlinien und erkennt Sicherheitsvorfälle automatisch: Mit einem MDM-System lassen sich automatisierte Updates und Patches ausrollen sowie einheitliche Sicherheitsrichtlinien und Compliance-Reporting umsetzen. Ein für alle Plattformen funktionierendes MDM-respektive gemäss Microsoft-Jargon ein UEM-System (Unified Endpoint Management) ist Microsoft Intune. Es gilt als einzig wirklich plattformübergreifendes UEM mit tiefer Microsoft-Integration, setzt allerdings Microsoft-Cloud-Lizenzen voraus. Ivanti UEM oder andere MDM-Lösungen wiederum kommen für iOS, MacOS und Android zum Einsatz.

### 4. Mobile Threat Defense (MTD)

Um Malware und Phishing auf Mobilgeräten proaktiv zu erkennen, benötigt es zudem eine effektive Mobile-Threat-Defense-Lösung wie etwa Microsoft Defender für Windows. Damit lassen sich auch MacOS, iOS und Android überwachen. Für Mobile Geräte wie Smartphones mit Android und iOS ist allerdings heute (noch) Lookout MES oder Zimperium zu empfehlen. Dies aus einfachem Grund, weil Microsoft-Technologie nicht vollständig mit Android- oder Apple-Geräten kompatibel ist und etabliertere MTD-Systeme Microsoft Defender aktuell noch weit überlegen sind. Lookout und andere Nicht-Microsoft-MTDs werden mit Microsoft Defender im Bedarfsfall mit Schnittstellen verbunden, erfassen Bedrohungen und leiten die nötigen Informationen dazu



Mitarbeitende arbeiten längst nicht mehr nur von einem Standort aus. Damit wird auch die IT-Infrastruktur immer heterogener und muss oft private Endgeräte und Netzwerke mit einschliessen.

an die SOC-Plattform respektive das SOC-Team weiter.

### Sicherheit in BYOD- und COPE-Szenarien

In modernen Arbeitsumgebungen ist BYOD (Bring Your Own Device) längst gängige Praxis: Mitarbeitende verwenden ihre privaten Geräte, um auf Unternehmensdaten zuzugreifen. Flexibilität und Produktivität steigen. Gleichzeitig erhöht sich aber auch das Risiko von Datenverlust, ungewollter Veröffentlichung und Sicherheitsverletzungen. Beim COPE-Modell (Corporate Owned, Privately Enabled) wiederum, bei dem das Unternehmen die Geräte bereitstellt, diese aber auch privat genutzt werden dürfen, bleibt die Herausforderung ähnlich: Geschäfts- und Privatnutzung müssen technisch und organisatorisch klar voneinander getrennt werden. Damit in beiden Fällen Sicherheit und Compliance gewährleistet bleiben, ist ein policy-basiertes Management und Containerisierung zentral: Der Schutz sensibler Unternehmensdaten basiert auf der konsequenten Trennung von privaten und geschäftlichen Bereichen auf dem Gerät. Richtlinien steuern, welche Apps auf Geschäftsdaten zugreifen dürfen, und verhindern den Transfer von Informationen zwischen privaten und geschäftlichen Domänen. Bei Android erfolgt mit Android Enterprise die Trennung über separate Benutzeroberflächen für Privat- und Arbeitsmodus. iOS und MacOS hingegen nutzen Container und App-basierte Zugriffsrechte mit unterschiedlichen Accounts. Unter Windows wird diese Trennung meist über separate Benutzerkonten innerhalb derselben Anwendung realisiert.

### Klare BYOD- und COPE-Richtlinien

Neben der technischen Absicherung ist eine verbindliche Unternehmensrichtlinie entscheidend. Sie regelt Verantwortlichkeiten, Nutzungsvorgaben, Datenschutz und Durchsetzungsmechanismen. Während bei BYOD der Einfluss des Arbeitgebers auf private Geräte begrenzt ist, hat das Unternehmen bei COPE volle Hoheit über Konfiguration, Sicherheitsrichtlinien und Monitoring – ein Vorteil besonders für Branchen wie Polizei oder Verwaltung, wo Erreichbarkeit und Datenschutz gleichermaßen kritisch sind.

### Weitere Massnahmen

Darüber hinaus sind starke Authentifizierung und Passwortrichtlinien Pflicht: Geräte müssen bereits bei der Registrierung mit Zwei-Faktor-Authentifizierung (2FA) abgesichert werden – etwa per Authenticator-App, PIN oder biometrischer Erkennung. Komplexe Passwörter und strenge Zugangsrichtlinien sind zwingend. Darüber hinaus ist auf einen segmentierten Zugriff und differenzierte Rechtevergabe zu achten. Denn nicht jede Benutzerrolle benötigt Zugriff auf dieselben Daten oder Systeme. Eine feingranulare Steuerung von Berechtigungen reduziert das Risiko interner Datenverletzungen.

Hinzu kommt ein aktives Schwachstellen- und Update-Management: Sowohl Betriebssysteme als auch Apps müssen regelmässig aktualisiert werden, um bekannte Sicherheitslücken zu schliessen. Die erwähnten Mobile Threat Defense (MTD)-Lösungen wie Lookout unterstützen dies auf iOS- und Android-Geräten

automatisch und warnen vor ausnutzbaren Schwachstellen. Denn selbst weit verbreitete Apps können Sicherheitslücken aufweisen. Solche Risiken können nur durch kontinuierliche Updates und MTD abgesichert werden.

### Vielfalt, Vernetzung und Expertise

Sichere, heterogene Netzwerke sind kein Widerspruch, sondern Konvergenz aus Technologie, Strategie und menschlichem Faktor. Entscheider sind gut beraten, auf Security-by-Design zu setzen. Das bedeutet, Sicherheitsrichtlinien und Zugriffsregeln müssen von Beginn an konsequent und systematisch automatisiert, rollenbasiert und für jede Umgebung passend in die Architektur eingebettet werden. Dieser Ansatz sorgt dafür, dass Anforderungen wie Zugriffsrechte, Compliance und Segmentierung nicht nachträglich, sondern schon beim Design der Infrastruktur und Prozesse berücksichtigt werden. So können Richtlinien plattformübergreifend und dynamisch umgesetzt werden und Sicherheitsstandards selbst bei Veränderungen wie neuen

Geräten oder Standorten automatisch erhalten bleiben. Ansonsten entstehen zahlreiche Risiken: Unternehmen sind anfällig für Sicherheitslücken, da Zugriffsrechte und Segmentierung oft lückenhaft und inkonsistent implementiert werden. Bei nachträglicher Integration treten häufig Compliance-Probleme auf, und es wird deutlich schwieriger, neue Geräte, Standorte oder Arbeitsweisen sicher einzubinden. Zudem steigen Aufwand und Kosten für das Nachrüsten und Patchen enorm, während die Angriffsflächen und das Schadenpotenzial unkontrolliert wachsen. Gemeinsam mit Kunden sollen deshalb Security-Konzepte kontinuierlich geprüft und weiterentwickelt werden. Dabei sollen nicht nur aktuelle Bedrohungen adressiert, sondern auch flexibel auf neue Angriffsvektoren reagiert werden. Entscheidend ist die Kombination aus klar definierten Richtlinien, konsequenter Geräteverwaltung und -schutz mit den für die jeweilige Umgebung passenden Technologien und intelligentem Sicherheitsmanagement. So lassen sich verteilte und mobile Arbeitsumgebungen sowohl flexibel als auch sicher gestalten.

### Mensch bleibt grösste Schwachstelle

Die technische Absicherung ist indes nur ein Teil der Lösung. Rund 80 Prozent der Angriffsszenarien nutzen den Faktor Mensch. Daher sind fortlaufende Awareness-Schulungen zu Social Engineering, Phishing und sicherem Umgang mit Endgeräten Pflicht: Sie umfassen rollenspezifische Trainings für IT und Business-User, simulierte Angriffsstübungen und Reporting-Funktionen und regelmässige Updates zu neuen Risiken und Best Practices. ■

#### DER AUTOR

Patrick Trevisan ist Mobile Security Consultant bei Nomasis. Das Unternehmen bietet in der Schweiz und Liechtenstein Lösungen für komplexe Netzwerksicherheits Herausforderungen, mit besonderem Fokus auf Mobile Security, Cloud Protection, Awareness und Zero Trust.



Entdecken Sie, wie  
Daten Ihren Erfolg  
vorantreiben können.

Besuchen Sie  
[www.dnb.com/de-ch](http://www.dnb.com/de-ch)

## MIT DER KRAFT VON DATEN UND ANALYSEN DIE ZUKUNFT ERSCHLIESSEN

In einer unberechenbaren Welt sind datengesteuerte Erkenntnisse der Schlüssel zu nachhaltigem Wachstum. Durch die Nutzung von KI-gestützten Plattformen und fortschrittlichen Analysen können Unternehmen Herausforderungen meistern, Chancen ergreifen und sich für die Zukunft wappnen.